APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,894	11/08/2001	Robert P. Basil	0960-021	4228

7590 09/22/2006		EXAMINER	
John L. Doughly		DOAN, TRANG T	
ARRIS International Inc.			
3871 Lakefield Drive		ART UNIT	PAPER NUMBER
Suwanee, GA 30024		2131	

DATE MAILED: 09/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 July 2006</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>09/26/2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This action is in response to the amendment filed on 07/05/2006.

2.   Claims 1-22 are pending. Claims 15 and 19 are amended.

Response to Arguments

1.   Applicant's arguments filed July 05, 2006 have been fully considered but they are

not persuasive.

On page 8-9 of the Remarks, Applicant has pointed out "one skilled in the art will

appreciate that the terms packet and frame describe portions of basic data elements of

digital communication". However these terms are not recited in the rejected claim (s) 1,

14, 15 or 19, therefore the examiner interprets each communication in the rejected

claim (s) 1, 14, 15 or 19 as each session for per communication. Although the claims

are interpreted in light of the specification, limitations from the specification are not read

into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir.

1993).

Furthermore to claims 1 and 14, applicant argues that Heer does not teach upon

each communication between the cable modem and head end, a new key is generated

and transmitted with the payload of the communication. The examiner disagrees with

applicant's arguments. Heer teaches a new session key is replaced each time there is

a new connection between the cable modem and the Head End (Heer: column 34 lines

12-42 and column 27 lines 34-59). One session could have one or more data

exchanges. I can interpret a communication as one data exchange. Each session

generates a new key for the cable modem and the head end to exchange data securely, and when the session end the new key is destroyed for security purpose. For the reason above, the examiner maintains the rejection.

In response to Applicant's argument that Heer does not disclose that a communication encrypted based on a key received in a previous communication from another device when one device sends a communication to the other as claimed in page 10 of the Remarks, examiner respectfully disagrees. Heer discloses a method of key exchange between the cable modem and the head end prior to a flow of information in column 27 lines 34-59. The examiner interprets the key exchange method of Heer as a key is exchanged between the cable modem and the head end prior to any transmission of data. Once the cable modem or the head end receives the key, the cable modem/head end uses the key to encrypt the communication among them.

Regarding to the arguments of claim 15 and 19 on page 10 of the Remarks, please refer back to the arguments of claims 1 and 14 above.

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2.   Claim s 1-2, 4, 11 and 14 rejected under 35 U.S.C. 102(e) as being anticipated

by Heer et al. (6028933) (hereinafter Heer).

3.   Referring to claims 1 and 14, Heer teaches:

A. the server receiving a scrambled upstream communication from a first client

modem (Heer: see figures 1 and 23, column 8 lines 40-52);

B. the server unscrambling a scrambled portion of the upstream communication

containing a new key for the first client modem using a previous seed for the first client

modem based on a previous key for the first client modem received in a previous

upstream communication from the first client modem (Heer: see figure 29, column 26

lines 1-67 and column 34 lines 12-23 and column 36 lines 40-67 and column 37 lines1-

15);

C. the server storing information sufficient to create a new seed for the first client

modem based on the new key for the first client modem based on the unscrambled

contents of the upstream communication (Heer: column 34 lines 24-41 and column 36

lines 40-67 and column 37 lines 1-15);

D. the server scrambling at least a portion of the next downstream

communication to a second client modem with scrambling based on a seed for the

second client modem based on a key for the second client modem, where in the key for

the second client modem is unrelated to the key for the first client modem (Heer: see

figure 1 (items 140a-c) column 26 lines 28-48);

E. the server scrambling at least a portion of the next downstream

communication to the first client modem with scrambling based on the new seed for the

first client modem based on the new key for the first client modem (Heer: column 34 lines 12-41 and column 36 lines 40-67 and column 37 lines 1-15);

F. the first client modem receiving the next downstream communication to the first client modem (Heer: see figure 2, column 8 lines 4-18);

G. the first client modem unscrambling the scrambled portion of the next downstream communication to the first client modem with the new seed for the first client modem based on the new key for the first client modem (Heer: column 8 lines 40-52 and column 26 lines 28-48);

H. the first client modem creating a next upstream communication containing a next key for the first client modem (Heer: see figure 31, column 26 lines 28-48 and column 36 lines 21-39);

I. the first client modem storing information sufficient to create a next seed for the first client modem based on the next key for the first client modem (Heer: column 34 lines 24-41 and column 36 lines 40-67 and column 37 lines 1-15); and

J. the first client modem scrambling at least a portion of the next upstream communication using the new seed for the first client modem based on the previously communicated new key for the first client modem (Heer: column 34 lines 12-41 and column 36 lines 16-39).

4.   Referring to claim 2, Heer teaches wherein the new seed for the first client modem equals the new key for the first client modem (Heer: column 26 lines 28-48).

5.   Referring to claim 4, Heer teaches wherein the new key for the first client modem

is a random number generated by the first client modem and not a transmission check

word (Heer: column 26 lines 49-66 and column 32 lines 12-16).

6.   Referring to claim 11, Heer teaches wherein a scrambled value is passed with

one communication and the value is used to alter the DVB randomization of the next

communication whereby the controlled variation in the DVB randomization provides a

layer of security to protect the next communication from an eavesdropper as the

eavesdropper would need the passed value in order to reverse the non-standard DVB

randomization (Heer: column 26 lines 28-48).

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

8.   Claims 3 and 5-6 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Heer in view of Rothenberg (5432850) (hereinafter Roth).

9.   Referring to claim 3, Heer does not explicitly disclose wherein the new key for the

first client modem is a transmission check word used for the purpose of testing the

accuracy of the upstream transmission, such that the new key for the first client modem

is transmitted with the upstream communication without adding to the overhead.

However, Roth teaches wherein the new key for the first client modem is a transmission

check word used for the purpose of testing the accuracy of the upstream transmission, such that the new key for the first client modem is transmitted with the upstream communication without adding to the overhead (Roth: column 3 lines 47-65 and column 4 lines 1-12).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Roth into Heer's invention for secure data transmission. The ordinary skilled person would have been motivated to make modification to Heer because adding a key to the data frame will help the receiver to decrypt the encrypted data sequence by employing the local address of the receiver as at least part of a decryption key (Roth: column 1 lines 40-44).

10.   . Referring to claim 5, Heer does not explicitly disclose wherein the scrambled portion of the upstream communication includes a portion of the data packet header. However, Roth teaches wherein the scrambled portion of the upstream communication includes a portion of the data packet header (Roth: column 3 lines 38-57).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Roth into Heer's invention for secure data transmission. The ordinary skilled person would have been motivated to make modification to Heer because encrypting a portion of the datagram's header will help the receiver to decrypt the encrypted data sequence by employing the local address of the receiver as at least part of a decryption key (Roth: column 1 lines 40-44).

11.   Referring to claim 6, Heer teaches wherein the scrambled portion of the upstream communication includes a field conveying the length of a variable length data packet (Heer: column 6 lines 53-67 and column 7 lines 1-61).

12.   Claims 7, 10 and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Heer in view of Jam et al. (5787483) (hereinafter Jam).

13.   Referring to claim 7, Heer does not explicitly disclose wherein first client modem unscrambles the scrambled portion of the next downstream communication to the first client modem with the new seed for the first client modem based on the new key for the first client modem only when a field in the next downstream communication lacks a signal to use a default seed based on a default key. However, Jam teaches wherein first client modem unscrambles the scrambled portion of the next downstream communication to the first client modem with the new seed for the first client modem based on the new key for the first client modem only when a field in the next downstream communication lacks a signal to use a default seed based on a default key (Jam: column 13 lines 50-57 and column 14 lines 1-67).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Jam into Heer's invention for secure data transmission. The ordinary skilled person would have been motivated to make modification to Heer because the field in the downstream communication provides the information of the key. Since the communication between transmitter and receiver uses changing keys, there is a need to synchronize the key between them.

14.   Referring to claim 10, Heer does not explicitly disclose the preliminary steps of

exchanging communications between the server and the first client modem, a portion of

the preliminary communications scrambled with a default seed until the server has

stored information sufficient to create an initial first client modem seed based on an

initial first client modem key. However, Jam teaches the preliminary steps of

exchanging communications between the server and the first client modem, a portion of

the preliminary communications scrambled with a default seed until the server has

stored information sufficient to create an initial first client modem seed based on an

initial first client modem key (Jam: column 13 lines 50-57 and column 14 lines 58-67).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have applied the teaching of Jam into Heer's invention for

secure data transmission. The ordinary skilled person would have been motivated to

make modification to Heer because the field in the downstream communication provides

the information of the key. Since the communication between transmitter and receiver

uses changing keys, there is a need to synchronize the key between them.

15.   Referring to claim 12, Heer does not explicitly disclose wherein: the server sent a

multicast address key and a multicast address in the next downstream communication

to the first client modem; the server sent the same multicast address key and the same

multicast address in the next downstream communication to the second client modem;

and further comprising the step of: the server creating a multicast communication

addressed to a multicast group comprising the first client modem and the second client

modem; the server sending the multicast communication after scrambling a portion of

the multicast communication with a seed based on the multicast address key. However,

Jam teaches the server sent a multicast address key and a multicast address in the

next downstream communication to the first client modem (Jam: column 14 lines 1-4

and lines 50-57); the server sent the same multicast address key and the same

multicast address in the next downstream communication to the second client modem

(Jam: column 14 lines 1-4 and lines 40-57); and further comprising the step of: the

server creating a multicast communication addressed to a multicast group comprising

the first client modem and the second client modem; the server sending the multicast

communication after scrambling a portion of the multicast communication with a seed

based on the multicast address key (Jam: column 24 lines 32-56).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have applied the teaching of Jam into Heer's invention for

secure data transmission. The ordinary skilled person would have been motivated to

make modification to Heer because in order to protect the communication, the data

must be encrypted. Only the right key can be able to decrypt the encrypted data, the

header of the data packet provides the information about the encryption/decryption key.

Since the communication between transmitter and receiver uses changing keys, there is

a need to synchronize the key between them.

16.   Referring to claim 13, Heer does not explicitly disclose wherein the server

scrambles at least a portion of the next downstream communication to the first client

modem with a seed based on both: the new key for the first client modem, and an

earlier key for the first client modem received before the new key for the first client

modem. However, Jam teaches wherein the server scrambles at least a portion of the

next downstream communication to the first client modem with a seed based on both:

the new key for the first client modem, and an earlier key for the first client modem

received before the new key for the first client modem (Jam: see figure 6(c) and column

14 lines 58-67).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have applied the teaching of Jam into Heer's invention for

secure data transmission. The ordinary skilled person would have been motivated to

make modification to Heer because in order to protect the communication, the data

must be encrypted. Only the right key can be able to decrypt the encrypted data, the

header of the data packet provides the information about the encryption/decryption key.

Since the communication between transmitter and receiver uses changing keys, there is

a need to synchronize the key between them.

17.   Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Heer in view of Jam and further in view of Roth.

18.   Referring to claim 8, Heer in view of Jam does not explicitly teach where the

default key is based on the address of the first client modem. However, Roth teaches

where the default key is based on the address of the first client modem (Roth: column 3

lines 47-57).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have applied the teaching of Roth into the combination of

Heer and Jam's invention for secure data transmission. The ordinary skilled person

would have been motivated to make modification to the combination of Heer and Jam

because the only station can get access into the encrypted data is the one that has the

right address. Without the right address, no one can decrypt the encrypted data to

prevent unauthorized stations attempting to access the data.

19.   Referring to claim 9, Heer in view of Jam does not explicitly teach wherein the

previous key for the first client modem received in a previous upstream communication

from the first client modem was sent with scrambling based on the default key.

However, Roth teaches wherein the previous key for the first client modem received in a

previous upstream communication from the first client modem was sent with scrambling

based on the default key (Roth: column 3 lines 47-57)

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have applied the teaching of Roth into the combination of

Heer and Jam's invention for secure data transmission. The ordinary skilled person

would have been motivated to make modification to the combination of Heer and Jam

because the only station can get access into the encrypted data is the one that has the

right address. Without the right address, no one can able to decrypt the encrypted data

to prevent unauthorized stations attempting to access the data.

20.   Claims 15 and 19-22 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Jam in view of Heer.

21.   Referring to claim 15, Jam teaches:

A. a server identifies the existence and the address of first client modem on a

shared transmission media (Jam: see figure 1, column 11 lines 24-29);

B. the server creates and transmits a downstream communication addressed to
the first client modem with a portion of the downstream communication scrambled twice
based on two default scrambling seeds, the downstream communication containing a
control field indicating that the default seeds were used (Jam: column 13 lines 59-67
and column 14 lines 1-7 and lines 58-67);

C. the first client modem receives the downstream communication and
recognizes that the default seeds were used (Jam: column 24 lines 32-56 and column
25 lines 19-30 and column 26 lines 17-25);

D. the first client modem unscrambles the downstream communication using the
default go seeds (Jam: see figure 3 and column 6 lines 17-65 and column 24 lines 45-
64 and column 25 lines 19-30);

E. the first client modem creates and transmits an upstream communication,
before transmission the upstream communication scrambled twice with the two default
seeds, the scrambled portion of the upstream communication containing a key created
by the first client modem (Jam: column 15 lines 34-58 and column 25 lines 19-30 and
column 26 lines 17-25);

F. the server receives the upstream communication and the server unscrambles
the scrambled portion of the upstream communication using the default seeds and
stores the key created by the first client modem (Jam: column 6 lines 17-22 and column
13 lines 50-53);

G. the server creates and transmits a downstream communication addressed to
the first client modem with the control field indicating that the communication is

scrambled using one default scrambling seed and one seed based on the key created

by the first client modem, a portion of the downstream communication scrambled once

with one default seed and once with one seed based on the key created by the first

client modem, the scrambled portion of the downstream communication including a key

created by the server for communication with the first client modem (Jam: column 6

lines 17-22 and column 14 lines 5-7);

H. the first client modem receives the downstream communication and reads the

control field (Jam: column 14 lines 5-7 and column 24 lines 42-64);

I. the first client modem unscrambles the downstream communication using the

one default seed and one seed based on the last transmitted key created by the first

client modem (Jam: see figure 3 and column 6 lines 17-65 and column 24 lines 45-64

and column 25 lines 19-30);

J. the first client modem stores the key created by the server for communication

with the first client modem (Jam: column 26 lines 12-25);

K. the first client modem creates and transmits an upstream communication,

before transmission a portion of the upstream communication including the new key

created by the first client modem is scrambled twice using the one seed based on the

last transmitted key created by the first client modem and one seed based on the last

transmitted server created key for communication with the first client modem (Jam:

column 15 lines 34-58 and column 25 lines 19-30 and column 26 lines 17-25);

L. the server receives the upstream communication, and unscrambles the

upstream communication using one seed based on the previously stored key created by

the first client modem and one seed based on the last transmitted server created key for communications with the first client modem (Jam: column 6 lines 17-22 and column 13 lines 50-53);

M. the server stores the last transmitted key created by the first client modem (Jam: column 26 lines 12-25);

N. the server creates and transmits a downstream communication addressed to the first client modem with the control field indicating that the communication is scrambled using one seed based on the last transmitted key created by the first client modem and one seed based on the last transmitted server created key for communication with the first client modem; a portion of the downstream communication scrambled once with one seed based on the last transmitted key created by the first client modem and once with one seed based on the last transmitted server created key for communication with the first client, the scrambled portion of the downstream communication containing a new server created key for communication with the first client modem (Jam: column 6 lines 17-22 and column 14 lines 5-7);

O. the first client modem receives the downstream communication and reads the control field (Jam: column 14 lines 5-7 and column 24 lines 42-64);

P. the first client modem unscrambles the downstream communication using one seed based on the previously stored server created key for communication with the first client modem and one seed based on the last transmitted key created by the first client modem (Jam: see figure 3 and column 6 lines 17-65 and column 24 lines 45-64 and column 25 lines 19-30);

Q. the first client modem stores the last transmitted server created key for

communication with the first client modem (Jam: column 26 lines 12-25),

REPEAT steps K through Q; UNTIL detecting a break in the communications

between the first client modem and the server; THEN GOTO Step B (Jam: column 18

lines 21-28 and column 38 lines 11-67 and column 39 lines1-2). Jam does not explicitly

disclose the double scrambling of communications sent to and from a particular client

modem. However, Heer teaches triple-DES encryption scheme can be used in the

encryption (Heer: column 2 lines 62-67 and column 3 lines 1-10 and column 26 lines 28-

48 and 61-66: triple-DES uses three different keys).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have applied the teaching of Heer into Jam's invention to

improve security and protect the transmitted data packets. The ordinary skilled person

would have been motivated to make modification to Jam because to prevent

unauthorized parties intercepting to the communication. Triple-DES encryption scheme

is used to ensure proper protection of the content of the data packet.

22.   Referring to claim 19, Jam teaches:

A. Unscramble the scrambled portion of the incoming communication with a

stored key created by the first device and a stored key created by the second device

(Jam: column 26 lines 12-25);

B. Store key created by the second device received in the scrambled portion of

the incoming communication (Jam: column 24 lines 30-56);

C. Create a new key created at the first device and include the new key in an

outgoing communication from the first device (Jam: column 14 lines 58-67 and column

15 lines 34-58 and column 25 lines 19-30, column 26 lines 17-25, column 34 lines 12-42

and column 27 lines 34-59);

D. Scramble portions of the outgoing communication including the new key

created by the first device with the stored key from the first device and the stored key

from the second device (Jam: column 15 lines 34-58 and column 25 lines 19-30 and

column 26 lines 17-25, column 34 lines 12-42 and column 27 lines 34-59);

E. Store key created by the first device (Jam: column 6 lines 17-22 and column

13 lines 50-53); and

F. Send outgoing communication (Jam: column 15 lines 9-58).

Jam does not explicitly disclose the dual key scrambling of communications sent

to and from a particular client modem. However, Heer teaches triple-DES encryption

scheme can be used in the encryption (Heer: column 2 lines 62-67 and column 3 lines

1-10 and column 26 lines 28-48 and 61-66: triple-DES uses three different keys).

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have applied the teaching of Heer into Jam's invention to

improve security and protect the transmitted data packets. The ordinary skilled person

would have been motivated to make modification to Jam because to prevent

unauthorized parties intercepting to the communication. Triple-DES encryption scheme

is used to ensure proper protection of the content of the data packet.

23.   Referring to claim 20, Jam in view of Heer teaches wherein: the stored key

created by the first device used in the scrambling and unscrambling operations is the

most recently stored key created by the first device, and the stored key created by the

second device used in the scrambling and unscrambling operations is the most recently

stored key created by the second device (Jam: column 26 lines 12-25).

24.   Referring to claim 21, Jam in view of Heer further teaches wherein the stored key

created by the first device used in the scrambling and unscrambling operations is not

the most recently stored key created by the first device (Jam: column 24 lines 42-56 and

column 25 lines 19-30 and column 26 lines17-25).

25.   Referring to claim 22, Jam in view of Heer further teaches wherein the stored key

created by the second device used in the scrambling and unscrambling operations is

not the most recently stored key created by the second device (Jam: column 24 lines

42-56 and column 25 lines 19-30 and column 26 lines17-25).

26.   Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Jam as in view of Heer, and further in view of Roth.

27.   Referring to claim 16, Jam in view of Heer does not explicitly disclose wherein

the key created by the first client modem is a transmission check word. However, Roth

teaches wherein the key created by the first client modem is a transmission check word

(Roth: column 3 lines 47-65 and column 4 lines 1-12).

        It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have applied the teaching of Roth into the combination of

Jam and Heer's invention for secure data transmission. The ordinary skilled person

would have been motivated to make modification to the combination of Jam and Heer because adding a key to the data frame will help the receiver to decrypt the encrypted data sequence by employing the local address of the receiver as at least part of a decryption key (Roth: column 1lines 40-44).

28.   Referring to claim 17, Jam in view of Heer in view of Roth further teaches wherein at least one of the default seeds is used solely for communications with the first client modem (Jam: column 13 lines 50-57).

29.   Referring to claim 18, Jam in view of Heer in view of Roth further teaches wherein at least one of the default seeds is derived from an address of the first client modem (Jam: column 24 lines 30-56).

Conclusion

30.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Trang Doan whose telephone number is (571) 272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Trang Doan
Examiner
Art Unit 2131

T.D.
September 15, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

9/18/06